REMARKS

Claims 1-3 and 14-28 are pending; and of these, claims 1 and 18 have been amended, and claims 20-28 have been cancelled without prejudice by this Amendment. Accordingly, claims 1-3 and 14-19 are presented for examination in this Amendment, which provides the required submission for the accompanying Request for Continued Examination. Applicants have also amended Fig. 3 of the Drawings, as well as the Abstract to conform to the claim amendments provided in the listing of claims above. In view thereof and the remarks below, reconsideration of the subject application is respectfully requested.

The Examiner has stated that Applicants have constructively elected the invention presented in claims 1-3 and 4-19 of the subject application, and that new claims 20-28, as presented in Applicants' Amendment dated November 29, 2007, are consequently withdrawn from consideration as being directed to a non-elected invention. As noted above, Applicants have cancelled claims 20-28, thereby obviating further consideration thereof.

The Examiner has rejected claims 1-3 and 4-19 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. In particular, the Examiner states that no disclosure exists with regard to "a receiving unit that receives a first or second command, the first command including information indicating one of a plurality of secret keys; a secret key setting unit that sets a first secret key indicated by the first command as a second secret key, if the first command is received by the receiving unit; and a digital signature generating unit that generates the digital signature the digital date using the second secret key, if a signature generating the second command is received receiving unit". Further, the Examiner states that "[t]here is no support in the written description that the first command indicates the first key", the limitation "that the digital signature generates by using the second key has no support . . ."

and that support could not be found for the limitation of "a secret key setting unit that sets a first secret key indicated by the first command as a second secret key, if the first command is received by the receiving unit."

The Examiner has further rejected claims 1-3 and 14-19 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner states that recitation in the claims of, "a receiving unit that receives a first or second command, the first command including information indicating one of plurality of secret keys; a secret key setting unit that sets a first secret key indicated by the first command as a second secret key, if the first command is received by the receiving unit, is "generally narrative and indefinite with the invention."

Applicants have amended their independent claim 1 to provide further clarification between the application as filed and the claims. In particular, Applicants take this opportunity to note that the recited feature of "a receiving unit" is supported at page 9, lines 5-24 and page 10, lines 3-15 and 19-27 of Applicants' specification as filed, that the feature of "a secret key changing unit" is supported at page 12, lines 6-17, and that the feature of "a digital signature generating unit" is supported at page 15, lines 8-27.

Applicants note that the above-listed section supporting the feature of the "receiving unit" provides that "[i]n the case of the key change command, the key number is of the secret key desired to be set in the IC card 10 is planted in the command data field 403." Applicants note further that the section supporting the "secret key changing unit" provides that "the secret key specified by the key change command is changed to the secret key used by the IC card 10. For example, if the key number specified by the key change command is No. 3, the secret key used by the IC card 10 is changed to the No. 3 secret key."

Applicants' above amendments are believed to appropriately address the Examiner's bases for rejection under 35 U.S.C. 112 as provided above, and therefore obviate further rejection of the claims under both 35 U.S.C. 112, first and second paragraphs. Accordingly, it is respectfully requested that the rejections be withdrawn.

The Examiner has again rejected Applicants' claims 1-3, as well as claims 14-19 presented in Applicants' most recent Amendment, under 35 USC 102(a) as being anticipated by Hirata, et al. (JP 2002-300150). Applicants have amended independent claim 1, and with respect to this claim, as amended, and its respective dependent claims, the Examiner's rejection is respectfully traversed.

Applicants' independent claim 1 has been amended to recite a digital signature generating apparatus that generates a digital signature of digital data, comprising a receiving unit that receives one of a first command and a second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus, a secret key changing unit that changes a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received by the receiving unit, and a digital signature generating unit that generates the digital signature of the digital data using the secret key specified by the first command, if the second command is received by the receiving unit.

The construction recited in Applicants' independent claim 1 is not taught or suggested by Hirata, et al. More particularly, there is no teaching or suggestion of the features of a receiving unit that receives one of a first command and a second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus, and a secret key changing unit that

changes a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received by the receiving unit.

Applicants have reviewed the Examiner's comments in the "Response to Arguments" section of the Office Action at page 5 thereof. There, in response to Applicants' remarks that Hirata, et al. fails to disclose a first feature of the key generation command "including information indicating one of plurality of secret keys," the Examiner maintains that Hirata, et al. does indeed teach this feature by stating that it "teaches this limitation . . . wherein IC card sends (first command) Secret key SK1 and Public key PK1 to key generation section in a card (paragraphs 0007), and thus it discloses that [the] first key [is] indicated by the first command." In response to Applicants' remarks that Hirata, et al. teaches a second feature of "setting the first key as a second secret key when the first key generation command [is] received by the apparatus," the Examiner argues that Hirata, et al. discloses "this limitation wherein the new key generation command [is] received by the card [and] then it changes to the new secret and public key SK2 and PK2 in place of SKI and PK1 (paragraphs 0003, 0008)."

As pointed out in their prior response, Applicants maintain that Hirata, et al. discloses merely an IC card which stores thereon a first secret key (SK1) and a first public key (PK1) corresponding to the first secret key. Abstract; Paragraph [0005]. When the IC card in Hirata, et al. receives a key generation command, a key generation section (11) of the IC card generates a new secret key (SK2) and a new public key (PK2), and a signature generating section (13) of the card generates a new signature using the first secret key (SK1) stored in the card. Abstract; Paragraph [0008]. Nonetheless, Applicants have amended their independent claim 1 with respect to each of the first and second features noted above.

In particular, Applicants have clarified independent claim 1 to recite "a receiving unit that receives one of a first command and a second command, the first command including

information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus." Hirata, et al. fails to teach or suggest this feature since there is no mention in Hirata, et al. of any command which is received by its IC card including information that indicates one of the plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus. This feature enables a selection from among a plurality of secret keys, and, as above stated, is realized and supported at page 10, lines 19-27 of Applicants' specification as filed, which provides that "[i]n the case of the key change command, the key number is of the secret key desired to be set in the IC card 10 is planted in the command data field 403."

In contrast, Hirata et al. mentions the sending and storing of only a single secret key, SK1, to the key generation section of the IC card. Abstract; Paragraph [0007]. However, this sending and storing is not a command, as the Examiner has argued, nor is what is sent include information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus. Moreover, there is no changing of the secret key to a secret key specified by a command including information indicating one of a plurality of secret keys. Instead, the secret key is changed in Hirata et al based on the key generation signal which does not include any secret keys and there is no changing of the secret key based on the receipt of the secret key SK1 in the key generation section.

Applicants' feature of a receiving unit that receives one of a first command and a second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus and further feature of a secret key changing unit that changes a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received by the receiving unit, are thus not taught or suggested by Hirata, et al.

Accordingly, Applicants' amended independent claim 1, and its respective dependent claims, which recite such features, in combination with the other elements as recited, thus patentably distinguish over Hirata, et al.

In view of the above, it is submitted that Applicant's claims, as amended, are in condition for allowance. Accordingly, reconsideration of the claims is respectfully requested.

Dated: May 29, 2008

Respectfully submitted,

COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200

Brian H. Buck
Reg. No. 48,776